IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION

TOMAS JONES, individually and on behalf of similarly situated individuals, **Plaintiff,** **v.** **HARRI (US), LLC** **Defendant.**	**Case No.**

CLASS ACTION COMPLAINT

Plaintiff Tomas Jones ("Jones" or "Plaintiff") individually and on behalf of all others similarly situated (the "Class"), by and through his attorneys, brings the following Class Action Complaint ("Complaint") pursuant to Rule 23 of the Federal Rules of Civil Procedure against Harri (US), LLC ("Harri" or "Defendant") its subsidiaries and affiliates, to redress and curtail its unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant Harri is a developer of workforce management solutions, including biometric timekeeping software and cloud-based time and attendance software products, which assist businesses in scheduling labor, managing employee time, and processing payroll.

2. Among the products Harri markets and sells is its biometric timeclock software, which "[u]tilize[s] cutting-edge facial recognition technology to streamline and secure [a client's]

workforce management,"[1] enabling its client employers to require that employees scan their facial geometry to track their time, attendance, and breaks. Defendant's software can be run on iOS and Android tablets and can integrate with a number of point-of-sale ("POS") and payroll systems such as Toast, Micros, ADP, and Paychex.

3. Harri markets and sells its software to a variety of different hospitality enterprises, including Steak 'n Shake ("SnS").

4. Plaintiff's employer, SnS, utilized Defendant's biometric timeclock software to require Plaintiff and others similarly situated to scan their facial geometry to track their time, attendance, and breaks.

5. Harri devices, like other biometric technology, authenticate user identities by capturing and utilizing their biometric identifiers and/or biometric information (collectively, "biometric data"). Harri's software allows devices, systems, and servers to communicate with one another.

6. When using Harri's facial recognition feature to record their time on Harri's biometric timeclock, workers scan their biometric identifiers, namely, their facial geometry. Once a user has enrolled or registered his or her facial geometry on the device, the device is able to identify them.

7. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – biometrics are unique, permanent biometric identifiers associated with each worker. This exposes Defendant's workers to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot,

[1] *See* Rethink The Time & Attendance Environment, *available at* https://harri.com/post-hire/time-attendance/ (last accessed Oct. 4, 2024).

MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, Facebook/Cambridge Analytica, and Suprema data breaches or misuses – workers have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

8. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendant's – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

9. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* https://www.opm.gov/cybersecurity/cybersecurity-incidents.

10. Take, for example, the Kronos data breach. Kronos, one of the world's leading providers of biometric timekeeping solutions, succumbed to a ransomware attack in December 2021. The resulting "administrative chaos" suffered by thousands of Kronos' corporate clients extended well into 2022. See Becky Sullivan, Hackers disrupt payroll for thousands of employers — including hospitals, (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933 /kronos-hack-lawsuits. And for the eight million workers whose personal data was exposed, it may be years before the true extent of their vulnerabilities come to pass. The system breached – Kronos Private Cloud – hosted Kronos's "Workforce Central," where employee biometric data collected for timekeeping purposes is stored.

11. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect and store Illinois citizens' biometrics, such as facial geometry.

12. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards its workers' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses workers' biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their facial geometry scans were being collected, stored, disseminated and used, as required by BIPA;

b. Develop and adhere to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' facial geometry scans, as required by BIPA;

c. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate or otherwise use their facial geometry scans, as required by BIPA; or

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their facial geometry scans to a third party as required by BIPA.

13. Accordingly, Plaintiff, on behalf of himself as well as the putative Class, seeks an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

14. Plaintiff Tomas Jones is a natural person and a resident of the State of Illinois.

15. Defendant Harri is a New York limited liability company that conducts business in the State of Illinois.

JURISDICTION AND VENUE

16. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)(A), (d)(5)(B) because the proposed class has 100 or more members, the amount in controversy exceeds $5,000,000.00, and the parties are minimally diverse.

17. This Court also has diversity jurisdiction under 28 U.S.C. § 1332(a) because the amount in controversy exceeds $75,000.00, and the parties are completely diverse.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to these claims occurred in this judicial district.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

19. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

20. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not

actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

21. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

22. BIPA was enacted due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. It does not, however, prohibit the appropriate use of biometric security and screening measures.

23. BIPA establishes a comprehensive baseline for biometric data protection by making it unlawful for a company to, among other things, collect, capture, store, share, or otherwise obtain, possess or disclose an individual's biometric data without:

a. developing, publishing, and adhering to a publicly available retention schedule with guidelines for permanently destroying biometric data;

b. obtaining a written release from each individual that notifies them, in writing, that their biometric data was being collected, stored, or otherwise obtained, and specifically why and for how long their biometric data would be collected, stored, and used;

c. obtaining an individuals informed consent before disclosing, redisclosing, or otherwise disseminating their biometrics to other private entities; and

d. protecting an individual's biometric data "using the reasonable standard of care within the private entity's industry" or "in a manner that is the same or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."

See 740 ILCS § 14/15(a), (b), (d), and (e).

24. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information. 740 ILCS § 14/15(c).

25. To ensure compliance, BIPA provides that, for each violation, individuals may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

26. Biometric identifiers include retina and iris scans, voiceprints, scans of hands and fingerprints, and – most importantly here – facial geometry scans. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

27. BIPA protects individuals' right to privacy over their biometrics the right to know the precise nature for which their biometrics are used, stored, protected, and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics, and creates a private right of action for lack of statutory compliance.

28. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendant Violates the Biometric Information Privacy Act

29. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using workers' biometric data as an authentication method stopped doing so.

30. However, Harri failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, Harri continues to collect, store, use and disseminate workers' biometric data in violation of BIPA.

31. Specifically, when workers first use a biometric timekeeping device integrated with Harri's cloud-based time and attendance software, they are required to have their biometric identifier (facial geometry) scanned, collected and stored in Harri database(s), where Harri collects and/or otherwise maintains workers' biometric data. Thereafter, Harri again collects and/or otherwise obtains workers' biometric data upon each subsequent scan of the workers' biometric identifier to clock-in and clock-out of work.

32. All biometric timekeeping devices capable of integration with Harri's cloud-based time and attendance software platforms are designed and constructed with a network interface, which provides for transmission of biometric data collected and/or obtained from those biometric timekeeping devices to Harri's servers and third-parties who host that data.[2]

33. Harri discloses workers' biometric data to third-parties, which receive, store, use, access, or otherwise process the biometric data for the purpose of providing their services, including the back-up of storage data.

34. Harri developed and markets a cloud-based time and attendance software platform, through which Harri actively manages, maintains, and stores data collected form integrated biometric timekeeping devices, including biometric data.

35. Harri accesses its biometric timekeeping servers for various purposes, including to provide support and payroll services for its clients.

[2] *See* Privacy Policy and Fair Processing Notice – US, *available at* https://harri.com/privacy/ (last accessed October 8, 2024), which states that Harri may share personal data "between our UK, USA and Ramallah entities, as well as with our advisors, affiliates, services providers, business partners and other third parties working with us in connection with our provision of services."

36. Harri fails to sufficiently inform workers enrolled with its cloud-based time and attendance software platforms: that Harri is collecting, obtaining., storing, disseminating, or using their biometric data; the extent or the purposes for which it does so; or to whom the data is disclosed.

37. Defendant Harri fails to sufficiently inform workers that, through its biometric timekeeping devices and cloud-based time and attendance software platforms, it collects, maintains, stores, disseminates, and uses their biometric data; fails to inform workers that it discloses their facial geometry data to other, currently unknown, third party web services providers, which host the biometric data in their data centers; fails to inform workers of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from workers before collecting, obtaining, and/or disseminating their biometric data.

38. Defendant also failed to develop and adhere to a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying workers' biometric data when the initial purpose for collecting or obtaining it is no longer relevant, as required by BIPA.

39. Because Harri has no publicly available retention schedule or destruction guidelines, Plaintiff has no reason to believe Defendant ever destroyed his or similarly situated workers' biometric data in accordance with BIPA, and in fact, believes the opposite.

40. Harri profits from the use of workers' biometric data. For instance, Harri markets and distributes its biometric timekeeping software and cloud-based time and attendance platforms to employers as a superior option to traditional timekeeping solutions because it leverages worker biometric identifier scans captured during punching for accurate time collection to help deter costly

"buddy punching"—where one worker punches in to or out of a time clock for another (absent) worker.[3]

41. Even more, Harri markets itself as an efficient tool for cutting HR costs because Harri provides automated data collection and analysis, as well as total integration between timekeeping software, cloud-based storage, and payroll service providers.

42. By marketing its biometric timekeeping devices in this manner, Harri obtains a competitive advantage over other time and attendance software and biometric verification companies, and secures profit from its use of biometric data, all while failing to comply with the minimum requirements for handling workers' biometric data established by BIPA.

43. The Pay By Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a biometric data but are not aware to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers such as a facial geometry scans, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long. Defendant disregards these obligations and their workers' statutory rights and instead unlawfully collect, store, use, and disseminate workers' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

44. Remarkably, Harri has created the same situation that Pay By Touch did by assembling a database of biometric data through broadly deployed biometric data readers and integrated, cloud-based time and attendance software platforms, but failed to comply with the law specifically designed to protect workers whose biometrics are collected in these circumstances.

[3] *See Rethinking Your Approach to Employee Time and Attendance*, Harri (June 26. 2023), available at: https://resources.harri.com/blog/rethinking-employee-time-attendance-hospitality-industry/.

Defendant disregards these obligations and workers' statutory rights and instead unlawfully collects, captures, obtains, stores, uses, and disseminates workers' biometric identifiers and information without ever receiving the workers' informed written consent, as required by BIPA.

45. Workers enrolled with Harri's biometric timekeeping devices and software (or who have their biometric data maintained or stored by Harri) are not told what might happen to their biometric data if and when Harri merges with another company, or worse, if and when Harri's business folds, or when the businesses of the other third parties that have received their biometric data fold.

46. Because Harri neither publishes a BIPA-mandated data retention policy nor discloses the purposes for their collection of biometric data, workers have no idea at the time of collection that Harri sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told at the time of collection to whom Harri currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.[4]

47. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

48. By and through the actions detailed above, Harri disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

[4] Harri all but confirms fears that such sensitive and personal information would be for sale in the event of a merger or bankruptcy, stating that "if all or substantially all of our business assets were acquired, or in the unlikely event that we go out of business or enter into bankruptcy, customer information would be one of the assets that is transferred or acquired by a third party." *See* Privacy Policy and Fair Processing Notice – US, *available a*t https://harri.com/privacy/ (last accessed October 8, 2024).

III. Plaintiff Tomas Jones's Experience

49. Plaintiff Tomas Jones worked as a Cook at Steak N' Shake ("SnS") from May 2024 through September 2024 in Tinley Park, Illinois.

50. Harri provides SnS with biometric time and attendance services, including a cloud-based time and attendance software platform. As part of its services, Harri hosts, collects, and manages the biometric data of Plaintiff and others working in Illinois using its biometric timekeeping software.

51. Plaintiff was required to scan his facial geometry on a device utilizing Harri's biometric timekeeping software as an authentication method for his time worked. Harri collected and/or otherwise obtained Plaintiff's biometric data upon Plaintiff's enrollment in Harri's biometric timekeeping software.

52. Plaintiff was required to scan his face geometry using SnS's Harri biometric timekeeping software onsite each time he: (1) began and ended his workday and (2) clocked in and out for breaks.

53. Harri subsequently collected and stored Plaintiff's biometric data in Harri's cloud-based database(s), maintained on Harri's hosted environments and servers, each time he scanned his facial geometry to clock-in or clock-out.

54. Harri did not obtain Plaintiff's consent before disclosing or disseminating his biometric data to third parties.[5]

[5] Harri defines "consent" as having created a Harri profile, which plainly does not comport with the requirements set out in BIPA, 740 ILCS § 14/15(d). *See* Privacy Policy and Fair Processing Notice – US, *available at* https://harri.com/privacy (last accessed October 8, 2024).

55. Harri did not properly inform Plaintiff in writing of the specific limited purpose(s) or length of time for which his facial geometry was being collected, obtained, stored, used, and/or disseminated.

56. Harri did not inform Plaintiff in writing or otherwise of the purpose(s) and length of time for which his facial geometry was being collected, did not obtain a written release from Plaintiff to collect, store, or use his facial geometry, did not develop and adhere to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's facial geometry, and did not obtain Plaintiff's consent before disclosing or disseminating his biometric data to third parties.

57. Plaintiff has never been provided with, nor ever signed, a written release allowing Harri to collect, capture, obtain, store, use, and/or disseminate his biometric data.

58. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's multiple violations of BIPA alleged herein.

59. No amount of time or money can compensate Plaintiff if his biometric data has been compromised by the lax procedures through which Defendant captures, stores, uses, and disseminates his and other similarly-situated individuals' biometrics. Moreover, Plaintiff would not have provided his biometric data to Defendant if he had known that Defendant would retain such information for an indefinite period of time without his consent.

60. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

61. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

62. Pursuant to Rule 23(a) and 23(b) of the Federal Rules of Civil Procedure, Plaintiff brings claims on his own behalf and as representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1 *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

63. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS 14/15.

64. Plaintiff seeks class certification for the following class of similarly-situated employees under BIPA:

> All individuals in the State of Illinois who had their biometric identifier(s) and/or biometric information collected, captured, received, stored or otherwise obtained or disclosed by Defendant during the applicable statutory period.

65. This action is properly maintained as a class action under Rule 23 because:

a. The class is so numerous that joinder of all members is impracticable;

b. There are questions of law or fact that are common to the Class;

c. The claims of Plaintiff are typical of the Class; and

d. Plaintiff will fairly and adequately protect the interests of the Class.

Numerosity

66. The total number of putative class members exceeds 100 individuals. The exact number of class members can easily be determined from Defendant's records.

Commonality

67. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff of its purposes for collecting, using, and storing his biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's biometric identifiers or biometric information;

D. Whether Defendant disclosed or re-disclosed Plaintiff's biometric identifiers or biometric information;

E. Whether Defendant sold, leased, traded, or otherwise profited from Plaintiff's biometric identifiers or biometric information;

F. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of its last interaction with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiff's facial geometry to identify him;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed recklessly or intentionally.

68. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

69. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

70. The claims asserted by Plaintiff are typical of the class members he seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

71. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to Rule 23(b)(3).

Predominance and Superiority

72. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy

because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

73. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant, and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/15(a): Failure to Institute, Maintain, and Adhere to Publicly-Available Retention Schedule

74. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

75. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

76. Defendant fails to comply with these BIPA mandates.

77. Defendant Harri is a New York limited liability company that conducts business in Illinois, and therefore, qualifies as a "private entity" under BIPA. 740 ILCS 14/10.

78. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry scans), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

79. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

80. Defendant failed to develop and adhere to a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

81. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and has not and will not destroy Plaintiff's or the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

82. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

83. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

84. BIPA requires companies to obtain informed written consent from individuals ***before*** acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] ***first***: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS § 14/15(b) (emphasis added).

85. Defendant fails to comply with these BIPA mandates.

86. Defendant is a New York limited liability company that conducts business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

87. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry scans), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

88. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

89. Defendant systematically and automatically collected, captured, or otherwise obtained Plaintiff's and the Class's biometric identifiers and/or biometric information without **first** obtaining the written release required by 740 ILCS § 14/15(b)(3).

90. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, or otherwise obtained, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, captured, or otherwise obtained, as required by 740 ILCS § 14/15(b)(1)-(2).

91. By collecting, capturing, and otherwise obtaining Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

92. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

93. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

94. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without obtaining consent for that disclosure. *See* 740 ILCS § 14/15(d)(1).

95. Defendant fails to comply with this BIPA mandate.

96. Defendant is a New York limited liability company that conducts business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

97. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry scans), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

98. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

99. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without obtaining the consent required by 740 ILCS § 14/15(d)(1).

100. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

101. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Jose Landa respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Tomas Jones as Class Representative, and appointing Stephan Zouras, LLC, as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Date: October 14, 2024

Respectfully Submitted,

/s/ Ryan F. Stephan
Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
STEPHAN ZOURAS, LLP
222 W. Adams Street,
Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com

jzouras@stephanzouras.com
aficzko@stephanzouras.com

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on October 14, 2024, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Ryan F. Stephan